Network Research Project

1. Installing applications

```
#!/bin/bash

# 1. Install relevant applications on the local computer
# Identify apps needed

function inst()
{
    #1) nipe (https://github.com/htrgouvea/nipe)
    git clone https://github.com/htrgouvea/nipe && cd nipe
    sudo cpan install Try::Tiny Config::Simple JSON
    sudo perl nipe.pl install
    #2) curl (https://www.cyberciti.biz/faq/how-to-install-curl-command-on-a-ubuntu-linux/)
    sudo apt install curl
    #3) geoiplookup (https://www.maketecheasier.com/ip-address-geolocation-lookups-linux/)
    sudo apt-get install geoip-bin
    #4) ssh (https://www.cyberciti.biz/faq/ubuntu-linux-install-openssh-server/)
    sudo apt-get install openssh-server
    #5) sshpass (https://www.tecmint.com/sshpass-non-interactive-ssh-login-shell-script-ssh-password/)
    sudo apt-get install sshpass
}
```

Installing applications required for the task on said Virtual Machine before moving forward with the task at hand.

1) nipe (https://github.com/htrgouvea/nipe)
   -used to make your linux anonymous via the Tor network
2) curl
   -used to extract the external IP from ifconfig.io
   (https://www.cyberciti.biz/faq/how-to-install-curl-command-on-a-ubuntu-linux/)
3) geoiplookup
   -used to look up a country tag to an IP address
   (https://www.maketecheasier.com/ip-address-geolocation-lookups-linux/)
4) ssh
   -used for creating a connection between two devices for remote access
   (https://www.cyberciti.biz/faq/ubuntu-linux-install-openssh-server/)
5) sshpass
   -SSH password automation
   (https://www.tecmint.com/sshpass-non-interactive-ssh-login-shell-script-ssh-password/)

Proof of Question 1:

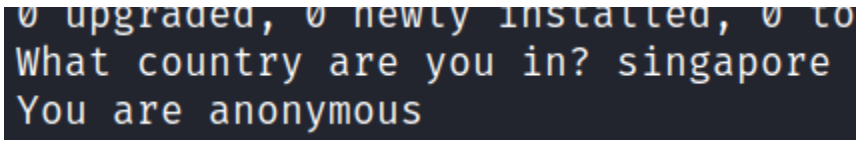
```
┌──(randy㉿kali)-[~]
└─$ bash project.sh
fatal: destination path 'nipe' already exists and is not an empty directory.
[sudo] password for randy:
Loading internal logger. Log::Log4perl recommended for better logging
Reading '/root/.cpan/Metadata'
  Database was generated on Thu, 14 Jul 2022 08:17:02 GMT
Try::Tiny is up to date (0.31).
Config::Simple is up to date (4.58).
JSON is up to date (4.07).
Can't open perl script "nipe.pl": No such file or directory
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
curl is already the newest version (7.83.1-2).
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab libllvm12 liblttng-ust-ctl4 liblttng-ust0 libperl5.32 libqt5quickwidgets5 libqt5webengine-data libqt5webengine5
  libqt5webenginecore5 libqt5webenginewidgets5 libre2-9 perl-modules-5.32 python3-ipaddr python3-pyqt5.qtquick python3-pyqt5.qtsql
  python3-pyqt5.qtwebchannel python3-pyqt5.qtwebengine python3-singledispatch python3-twisted-bin
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 167 not upgraded.
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
geoip-bin is already the newest version (1.6.12-8).
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab libllvm12 liblttng-ust-ctl4 liblttng-ust0 libperl5.32 libqt5quickwidgets5 libqt5webengine-data libqt5webengine5
  libqt5webenginecore5 libqt5webenginewidgets5 libre2-9 perl-modules-5.32 python3-ipaddr python3-pyqt5.qtquick python3-pyqt5.qtsql
  python3-pyqt5.qtwebchannel python3-pyqt5.qtwebengine python3-singledispatch python3-twisted-bin
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 167 not upgraded.
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
openssh-server is already the newest version (1:9.0p1-1+b1).
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab libllvm12 liblttng-ust-ctl4 liblttng-ust0 libperl5.32 libqt5quickwidgets5 libqt5webengine-data libqt5webengine5
  libqt5webenginecore5 libqt5webenginewidgets5 libre2-9 perl-modules-5.32 python3-ipaddr python3-pyqt5.qtquick python3-pyqt5.qtsql
  python3-pyqt5.qtwebchannel python3-pyqt5.qtwebengine python3-singledispatch python3-twisted-bin
Use 'sudo apt autoremove' to remove them.
```

2. Check if the connection is anonymous

```
24  # 2. Check if the connection is from your origin country. If no, continue.
25  function anon()
26  {
27      function anonchecker()
28      {
29      read -p "What country are you in? " country
30      user=$(whoami)
31      ip=$(curl -s ifconfig.co)
32      current=$(geoiplookup "$ip" | awk '{print $NF}')
33      #checking case insensitive in while statement(https://stackoverflow.com/questions/1728683/case-insensitive-comparison-of-strings-in-shell-script)
34      if [ "${current,,}" == "${country,,}" ]
35      then
36          echo "You are exposed"
37      else
38          echo "You are anonymous"
39      fi
40      }
41      anonchecker
42      var=$(anonchecker)
43      while [ "$var" == "You are exposed" ]
44      do
45          cd /home/$user/nipe
46          sudo perl nipe.pl restart
47          ip2=$(sudo perl nipe.pl status | grep Ip | awk '{print $NF}')
48          current=$(geoiplookup "$ip2" | awk '{print $NF}')
49          anonchecker
50          var=$(anonchecker)
51      done
52  }
```

Checking if I'm currently anonymous via cross-referencing country you are currently in.

Proof of Question 2:



3. Connect automatically to the VPS and execute tasks

```
51
52  function vps()
53  {
54      ip=$(curl -s ifconfig.co)
55      #Installing app(https://www.kali.org/tools/whois/)
56      apt install whois
57      whois "$ip"
58      #Installing app(https://installati.one/kalilinux/nmap/)
59      apt-get -y install nmap
60      nmap "$ip"
61  }
62
63  inst
64  anon
65  #sshpass (https://stackoverflow.com/questions/22107610/shell-script-run-function-from-script-over-ssh)
66  sshpass -p P@s5w0Rd ssh root@134.209.110.3 "$(typeset -f vps); vps"
67
```

Running task via ssh through a function from current machine.
Proof of Question 3:
Running Whois

```
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Reading package lists ...
Building dependency tree ...
Reading state information ...
whois is already the newest version (5.5.6).
0 upgraded, 0 newly installed, 0 to remove and 89 not upgraded.

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2022, American Registry for Internet Numbers, Ltd.
#


NetRange:       134.209.0.0 - 134.209.255.255
CIDR:           134.209.0.0/16
NetName:        DIGITALOCEAN-134-209-0-0
NetHandle:      NET-134-209-0-0-1
Parent:         NET134 (NET-134-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS14061
Organization:   DigitalOcean, LLC (DO-13)
RegDate:        2018-10-18
Updated:        2020-04-03
Comment:        Routing and Peering Policy can be found at https://www.as14061.net
Comment:
Comment:        Please submit abuse reports at https://www.digitalocean.com/company/contact/#abuse
Ref:            https://rdap.arin.net/registry/ip/134.209.0.0
```

Running Nmap Scan

```
# Copyright 1997-2022, American Registry for Internet Numbers, Lt
#

Reading package lists ...
Building dependency tree ...
Reading state information ...
nmap is already the newest version (7.80+dfsg1-2build1).
0 upgraded, 0 newly installed, 0 to remove and 89 not upgraded.
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-14 15:37 UTC
Nmap scan report for randall-network-project (134.209.110.3)
Host is up (0.0000050s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```